Academy *for*
Collaborative
Education *of* Brussels

# DATA PROTECTION, PRIVACY AND RETENTION POLICY

Last updated : August 2022

## 1. Objective

The aim of this Data Protection and Privacy Policy (hereinafter: “this Policy”) is to provide adequate safeguards for the processing of personal data (as defined below) by ACE of Brussels (Academy for Collaborative Education of Brussels), Drève du Prieuré 19, 1160 Auderghem (Brussels) (hereafter “ACE of Brussels” or “we”).

This Policy provides all relevant information and instructions for anyone within ACE of Brussels who, in the performance of his role, processes personal data as defined under the policy, and this next to other relevant policies in this respect. Ace of Brussels wishes to be completely transparent with regard to the processing of Personal Data and therefore, we have presented below all the information you may need on this subject.

This Policy is drafted in order to ensure compliance with the European Regulation 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, or GDPR) and applicable local legislation.

This policy does not aim to provide a stronger protection than required by the applicable legislation.

Please take a little of your time to read this Policy to understand the data processing operations carried out by ACE of Brussels.

ACE of Brussels reserves the right to make changes to this Policy from time to time, for example in the light of new developments, or new legislation. ACE of Brussels will always inform you of such changes in advance. In any event, it is recommended that you consult this Policy regularly.

## 2. For whom?

This policy has been written for any and all people who, in the performance of their role within ACE of Brussels, process personal data of data subjects as defined in this policy.

Examples of data subjects are:

- Current personnel
- Potential personnel (job applicants)
- Former personnel
- Employees’ family members
- Students
- Contractors/consultants/freelancers
- Temporary agency workers
- Directors and shareholders
- Contact persons with customers
- Contact persons with suppliers
- Visitors of the ACE OF BRUSSELS’ premises
- Prospects
- And so on

This Policy is relevant for any department where personal data are processed.

## 3. Scope

This Policy applies to the processing of personal data in the context of ACE of Brussels’ activities.

## 4. Definitions

The GDPR includes a list of definitions, the most important ones will be explained below:

- **"Controller"** means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. In the context of this Policy, ACE OF BRUSSELS is considered as the Controller;
- **"Employee"** – For practical reasons, the word "employee" will have a broad scope in this policy and will include any current or former employee, temporary (agency) worker, volunteer, expat, intern or other non-permanent employee or worker;
- **"European Economic Area** ("**EEA**")" currently including the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK;
- **"Personal data"** means any information relating to an identified or identifiable natural person ("data subject");
- **"Data subject"** means an identifiable person who can be identified either directly or indirectly, in particular by reference to an identifier such as a name, an ID number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- "**Sensitive personal data**" means Personal Data revealing a person's:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade-union membership;
  - data concerning health or sex;
  - data relating to criminal convictions and offences or related security measures;
- **"Processing"** is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." This means that the term "processing" has a very broad scope;
- **"Data Protection Requirements"** means the Directive, the GDPR, Local Data Protection Laws, any subordinate legislation and regulation implementing the GDPR, and all Privacy Laws;
- **"Directive"** means the EU Data Protection Directive 95/46/EC (as amended);
- **"GDPR"** (General Data Protection Regulation) means the European Union Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- **"Local Data Protection Laws"** means any subordinate legislation and regulation implementing the Directive or the General Data Protection Regulation which may apply to the Agreement;
- **"Privacy Laws"** means all applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion, and text messaging, email, and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data;
- **"Data breach"** is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

## 5. WHY DOES ACE OF BRUSSELS USE PERSONAL DATA?

ACE of Brussels collects personal data, including special categories of personal data of the data subjects quoted above, especially to provide a safe and caring international environment for teaching, learning and general educational purposes.

More specifically we process your personal data for the following purposes, and other purposes that are compatible with those described below:

- to undertake and manage the school admissions and enrolment;
- to provide a safe and secure learning environment;
- to comply with child protection requirements;
- to support and enable the academic and personal objectives of children, including the monitoring and reporting of progress;

- to provide our educational services;
- to provide support and care for emotional and psychological wellbeing;
- to protect the health of the students and staff;
- to provide a tailored learning environment and make evidence based education decisions for the children we serve;
- to support and develop our employees in the performance of their duties;
- for financial planning, to help in the future planning and resource investment purposes;
- to meet our statutory reporting requirements to the education and other authorities;
- to help investigate any concerns or complaints you may have;
- to make you aware and inform you about our services, news, events and activities that are undertaken at or in association with ACE of Brussels;
- to communicate with you within the framework of your relationship with ACE of Brussels;
- to ensure the safety and security at ACE of Brussels, including camera surveillance;
- for forecasting and planning for education service provision;
- to respond to requests of our staff, (former) students or authorities regarding historic information pertaining to their time at ACE of Brussels.

## 6. Principles for processing personal data

ACE of Brussels respects the privacy of the data subjects referred to above whose personal data it processes and is committed to protecting their personal data in compliance with the GDPR. This compliance is consistent with ACE of Brussels' desire to keep its employees and any and all other data subjects informed about the processing of their personal data, and to recognise and respect their privacy rights.

ACE of Brussels will observe the following principles when processing personal data:

- The data will be processed *lawfully*, *fairly* and in a *transparent* manner in relation to the data subject;
- The data will be collected for *specified, legitimate purposes*; the data will not be processed further in ways that would be incompatible with those purposes;
- The data will be *adequate, relevant to and limited to* the purposes for which they are processed;
- The data will be *accurate* and, where necessary kept up *up-to-date*. Reasonable steps will be taken to *rectify or delete* any data that is inaccurate or incomplete;
- The data will be *kept only as long as it is necessary* for the purposes for which it was collected and processed. Those purposes shall be described in this Policy;
- The data will be *deleted or amended* following a justified request by the data subject;
- The data will be processed in accordance with the *individual's legal rights* as described in this Policy or as provided by law;
- Appropriate *technical, physical and organisational measures* will be taken to prevent unauthorised access, unlawful processing and unauthorised or accidental loss, destruction or damage to data. In case of any violation as referred to in the previous sentence, and/or in case of any accidental data leak, ACE of Brussels will take appropriate steps to end the violation/eliminate the leak and determine liabilities in accordance with the GDPR and will cooperate with the competent authorities where necessary, should they be involved as a result of such violation or leak.

## 7. Personal data processed by ACE of Brussels

Personal data is a very broad concept, which calls for a wide interpretation. Whenever a natural person, irrespective of the category can potentially be identified based on the data which are processed in ACE of Brussels' systems or applications or in manual files, the Data Protection Requirements apply.

Types of personal data which in itself or by combination allow singling out a natural person are for example:

- identification data (name, address, phone number, e-mail address,);
- pictures/images;
- video images;
- financial specifics;
- personal characteristics (such as age, gender, date of birth, place of birth, civil status, nationality);

- physical or psychological data;
- living and consumer habits;
- data on family;
- data on training and employment;
- special categories of data (such as health information, background);
- educational and evaluation data (such as assessments, relevant medical information, special educational needs information, behavioural information);
- attendance information (such as sessions attended, number of absences and absence reasons);
- logging and audit in the use of IT systems and education technology apps, applications and cloud-based systems;
- communication and correspondence data (such as emails, letters and other types of correspondence).

Basically, any information about an individual is personal data. However, not all these data can actually lead to the unique identification of an individual – and this is, in essence, how personal data is defined under the Data Protection Requirements. For example, if you only have the name and gender of a person, this will not be sufficient to single out someone from the whole of a country's population but may achieve identification within the school.

To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, taking into account the costs of and the amount of time required for identification, the available technology at the time of the processing and technological developments (e.g. the combination of a position and a company without a name will take a couple of minutes online to identify - for example based on LinkedIn - who it is about).

The Data Protection Requirements do not apply to anonymous information.

Given the fact that the Data Protection Requirements only apply to natural persons, data on legal persons is also out of scope, unless it allows identifying a natural person.

The education services we provide require us to collect and process special categories of data, such as health information, for example for the purposes of safeguarding the protection of the students (and employees) and the wellbeing of those within our care. We do not disclose or share special categories of data without explicit and unambiguous consent, unless we have to do so where we are required to by law, or where we have good reason in protecting the vital interests of an individual, or where not doing so would place someone else at risk.

## 8. Information on the processing of personal data under ACE of Brussels' responsibility

To process personal data ACE of Brussels must rely on a legal basis.

ACE of Brussels will process personal data in a lawful way based on one of the following (relevant) legal grounds:

- because it is **necessary** for the **performance of a contract** to which the data subject is party or in order to take steps **at the request** of the data subject **prior to entering into a contract,** e.g. the employment contract with employees;
- because it is **necessary** for compliance with a **legal obligation** to which ACE of Brussels is subject;
- because it is **necessary** for the purposes of the **legitimate interests** pursued by ACE of Brussels or by a **third party**, **except** where such interests are **overridden** by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
    - ⇨ This latter legal basis, which will have to be used a lot, therefore requires carrying out a **balancing test** between the interests of ACE of Brussels on the one hand and the persons whose data are processed on the other hand.

ACE of Brussels might also make use of other legal grounds, but these are less relevant:

- When the data subject has given its free, specific, informed and unambiguous **consent** to the processing of his or her personal data for one or more specific purposes;

⇨ In cases where there is a real or potential relevant prejudice that arises from a data subject not consenting, then consent is not valid since it is not and cannot be freely given (e.g. during employment relationship);

- When the processing is **necessary** in order to protect the **vital interests** of the data subject or of another natural person (which should be interpreted in a limited way) e.g. in case of a medical urgency.

As a principle, for each specific processing activity, ACE of Brussels will rely on only one legal ground.

Occasionally ACE of Brussels might have to process sensitive personal data, e.g. in the context of the employment relationship. Please note that the processing of **Sensitive personal data** is in principle prohibited. Limited exceptions exist such as:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the law provides that the prohibition may not be lifted by the data subject (which is often the case in the employment relationship where several local laws provide that consent can only be given if the employee acquires an advantage);
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of ACE of Brussels or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by law or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c) processing relates to personal data which are manifestly made public by the data subject;
d) processing is necessary for the establishment, exercise or defence of legal claims;
e) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of the law or pursuant to contract with a health professional and under the responsibility of a professional subject to the obligation of professional secrecy.

For more information on the categories of personal data and the purposes for which these data are processed, ACE of Brussels refers to:

- the privacy notice for employees;
- the privacy notice for students and their parents;
- the privacy statement on the website.

## 9. SECURITY/CONFIDENTIALITY

ACE of Brussels is committed to taking appropriate technical, physical and organisational measures to protect personal data against unauthorised access, unlawful processing, accidental loss or damage and unauthorised destruction.

### 9.1. Equipment and Information Security

In order to safeguard against unauthorised access to personal data by third parties, ACE of Brussels is taking all possible measures to maintain all electronic personal data held by ACE of Brussels on systems that are protected by up-to-date secure network architectures that contain firewalls and intrusion detection devices. The data are saved in servers that are “backed up” to avoid the consequences of any inadvertent erasure, destruction or loss otherwise. The servers are stored in facilities with high security, access protected to unauthorised personnel, fire detection and response systems. The location of these servers is known to a limited number of ACE of Brussels’ employees.

### 9.2. Access security

The importance of security for all personal data associated with ACE of Brussels’ employees is of highest concern. ACE of Brussels is committed to safeguarding the integrity of personal information and preventing unauthorised access to information maintained in ACE of Brussels’ databases. These measures are designed and intended to prevent corruption of data, block unknown and unauthorised access to our computerised system and information, and to provide reasonable protection of personal data in ACE of Brussels’ possession. All employee and student files are confidentially maintained in the principal’s office in secured and locked file cabinets or rooms. Access to the computerised database is controlled by a log-in sequence and requires users to identify themselves and provide a password before access is granted. Users are limited to data required to perform their job function. Security features of our

software and developed processes are used to protect personal information from loss, misuse, and unauthorised access, disclosure, alteration, and destruction.

### 9.3. Training

ACE of Brussels will be responsible for conducting adequate training sessions regarding the lawful, enumerated intended purposes of processing personal data, the need to protect and keep information accurate and up-to-date, the lawful purposes of collecting, handling and processing data that is transferred from the EEA to a third country and the need to maintain the confidentiality of the data to which employees have access. Authorised users will comply with this Policy and ACE of Brussels will take appropriate actions in accordance with applicable law, if Personal Data are accessed, processed, or used in any way that is inconsistent with the requirements of this Policy.

## 10. Data Protection by Design and By Default

### 10.1. General principle

While working on new initiatives or ongoing projects (business initiatives, new systems, tools or applications) ACE of Brussels has a responsibility to ensure data protection requirements are integrated from the design stage (so-called “Privacy by Design”) to the operation (so-called “Privacy by Default”). Furthermore, ACE of Brussels needs to ensure and be able to demonstrate that data is processed in accordance with the Data Protection Requirements.

### 10.2. Data Protection Impact Assessment (DPIA)

Where processing operations are likely to result in a high risk to the rights and freedoms of persons, ACE of Brussels will carry out a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment will be taken into account when determining the appropriate measures to be taken. Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the Supervisory Authority should take place prior to the processing.

In general, ACE of Brussels can consider that a processing meeting 2 of the 9 criteria below would require a DPIA to be carried out:

(1) Evaluation or scoring, including profiling and predicting, especially from “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements”;
(2) Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person”;
(3) Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area”;
(4) Sensitive data or data of a highly personal nature;
(5) Data processed on a large scale;
(6) Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject;
(7) Data concerning vulnerable data subjects, such as employees;
(8) Innovative use or applying new technological or organisational solutions, like combining use of fingerprint and face recognition for improved physical access control, etc.;
(9) When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”.

Local Supervisory Authorities may establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant. These lists can be consulted here for Belgium: https://www.dataprotectionauthority.be/

## 11. Rights of data subjects

### 11.1. Procedure

ACE of Brussels shall facilitate the exercise of data subject rights whose personal data it processes as a controller. Data subject requests will be handled by our Mrs Jackie Daire (info@aceofbrussels.com).

Where ACE of Brussels has reasonable doubts concerning the identity of the natural person making the request referred to in these clauses, ACE of Brussels may request the provision of additional information necessary to confirm the identity of the data subject.

ACE of Brussels shall provide information on action taken on a request under these clauses to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. ACE of Brussels shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Any actions taken under these clauses shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, ACE of Brussels may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

### 11.2 Which rights?

Data subjects have a right to:

a) **Access and copy of personal data**: obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information referred to above. ACE of Brussels shall also provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, ACE of Brussels may charge a reasonable fee based on administrative costs.

   This right can not affect the rights and freedoms of others. Information relating to other natural persons can therefore no be (fully) accessed or copied. ACE of Brussels' rights should also not be affected (e.g. ACE of Brussels can not be obliged to provide confidential business information).

b) **Have personal data rectified**: obtain without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

c) **Have personal data erased**: a data subject can request ACE of Brussel to delete data in one of the following cases:

   (1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
   (2) the data subject withdraws consent on which the processing is based on consent, and where there is no other legal ground for the processing,

(3) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes, (4) the personal data have been unlawfully processed, or
(5) the personal data have to be erased for compliance with a legal obligation.

This right to erasure shall not apply to the extent that processing is necessary:
(1) for exercising the right of freedom of expression and information,
(2) for compliance with a legal obligation, or
(3) for the establishment, exercise or defence of legal claims.

**d) Withdraw consent:** if ACE of Brussels has relied only on consent as a ground for processing, the data subject may withdraw consent at any time. However, this will not affect the lawfulness of any processing activities before such withdrawal;

e) **Restrict the processing of personal data**, for instance if the accuracy of the personal data is contested;

f) **Data portability**: a data subject can receive the personal data concerning him or her, which he or she has provided to ACE of Brussels, in a structured, commonly used and machine-readable format and have the right to transmit those data without hindrance from ACE of Brussels where the processing is based on consent or on a contract and the processing is carried out by automated means. This right can not affect other person's rights and freedoms.

g) **Object to processing of personal data** concerning him or her which is based on the legitimate interests, including profiling based on those provisions or processing for direct marketing purposes. In case of a justified objection, ACE of Brussels will immediately have to cease the processing unless there are compelling grounds for the processing or where ACE of Brussels needs the data for the establishment, exercise or defence of legal claims.

h) **Not to be subject to automated decision making**, i.e. a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless authorised by law or necessary for entering into, or performance of, a contract, in which case at least the right to obtain human intervention on the part of ACE of Brussels should be provided.

If a data subject has complaints relating to the processing of their personal data, the data subject should raise these in the first instance with the ACE of Brussels' Mrs Jackie Daire (info@aceofbrussels.com), as mentioned in the different privacy notices.

Alternatively, the data subject may also raise complaints with the Supervisory Authority:

Data Protection Authority
Rue de la Presse 35, 1000 Brussels
contact@apd-gba.be
https://www.dataprotectionauthority.be/

## 12. Retention of personal data

ACE of Brussels will generally hold personal data for as long as it is necessary for the purposes they are being processed for. For that purpose, ACE of Brussels has developed a Data Retention Policy, based on the processing activities it recorded. An overview of the relevant retention periods taking into account legal minimum and maximum retention periods and statutes of limitations. This Data Retention Policy is included in this Data Protection and Privacy Policy. Every employee who has control of data or records, including data or records created or received and subsequently processed by this employee, e-mails sent and received, e-mails in their archive, records in their personal drive and records they have uploaded to shared drives, is responsible for compliance with this Data Retention Policy and should therefore delete the data or records as soon as the applicable retention period has expired.

## 1. Transfer of personal data

Personal data might be disclosed to third party service providers outside ACE of Brussels if disclosure is consistent with a ground for processing on which ACE of Brussels rely and doing so is lawful and fair to the data subject. More specifically, ACE of Brussels may disclose the data of a data subject if it is necessary for its legitimate interests as a company or the interests of a third party (but ACE of Brussels will not do this if these interests are over-ridden by the privacy rights of the data subject).

More specifically, this includes for example the following categories of recipients:

- Schools, colleges or universities that the students attend after leaving ACE of Brussels;
- Local education authorities in Brussels;
- Nurses, doctors or social service organisations (amongst others where sharing is in the vital interests, or where not sharing could have a negative impact on the individual);
- Providers of information systems that are necessary for ACE of Brussels to deliver the admissions, administration, teaching and learning, and child protection services;
- Providers of IT hosting and maintenance services.

ACE of Brussels may also disclose personal data:
- if the data subject gives his/her consent;
- where we are required to do so by law; and
- in connection with criminal or regulatory investigations.

Where disclosure to a third-party service provider is necessary, ACE of Brussels shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. There will be contracts in place between ACE of Brussels and any such third-party service provider in line with the GDPR.

## 14. Automated decisions

Automated decisions are defined as decisions about individuals that are based solely on the automated processing of data and that produce legal effects or that significantly affect the individuals involved.

As a rule, ACE of Brussels does not make automated decisions. If automated decisions are made, affected persons will be given the opportunity to express their views on the automated decision in question and object to it.

## 15. Data breaches

### 15.1. Reporting data breaches

Care should be taken by anyone who, in the performance of his/her activities at ACE of Brussels, processes personal data (of students, family of the students, colleagues, job applicants, business partners, third parties, and so on) to prevent incidents (either accidentally or deliberately) that could compromise the privacy of the data subjects involved.

In the event of a data breach as defined below and in the list of definitions in this General Privacy Policy, it is vital that appropriate actions are taken as soon as possible to minimise the risk of damage to the person involved and, in the end, also to ACE of Brussels itself (reputational, imposed penalties, …).

ACE of Brussels should immediately notify the relevant national Supervisory Authority of any personal data breach that has or is likely to have serious negative consequences for the protection of personal data. ACE of Brussels should notify the Supervisory Authority within 72 hours after becoming aware of the personal data breach. In some cases, ACE of Brussels should also inform the data subject(s) affected by the personal data breach.

### 15.2. What is a data breach?

A breach is a type of security incident. However, the documentation and notification requirement under the Data Protection Requirements only applies where there is a breach of personal data.

In general, data breaches can be categorised according to the following principles:

- ***"Confidentiality breach"*** - where there is an unauthorised or accidental disclosure of, or access to, personal data;
- ***"Availability breach"*** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data;
- ***"Integrity breach"*** - where there is an unauthorised or accidental alteration of personal data.

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these. Just think of an ACE of Brussels employee whose laptop, on which personal data is stored, is stolen, or of an e-mail containing personal data which is accidentally sent to the wrong address.

**1.3. Internal reporting**

All individuals who access, use or manage ACE of Brussels' information are responsible for reporting any security breach and information security incidents immediately to the Data Protection Officer so it can be assessed immediately if the breach needs reporting or not.

The report should include full and accurate details of the incident, including who is reporting the incident, what type of incident it is, if the data relates to people, and how many people are involved. A breach notification form for this purpose can be found on the intranet.

The contact details for the reporting are info@aceofbrussels.com.

**1.4. Investigation and Risk Assessment**

Depending on the type of incident, ACE of Brussels will investigate the incident. An investigation will start within 24 hours of the incident being reported, where possible.

The investigation will establish the nature of the incident, the type of data involved, and whether personal data are involved (and if yes, who the data subjects are and how many personal records were breached).

The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident, for instance whether harm could come to individuals, or whether data access or IT services are disrupted.

**1.5. Containment and Recovery**

The Data Protection Officer will determine the appropriate course of action and the resources required to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down certain equipment.

Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data, and changing compromised passwords.

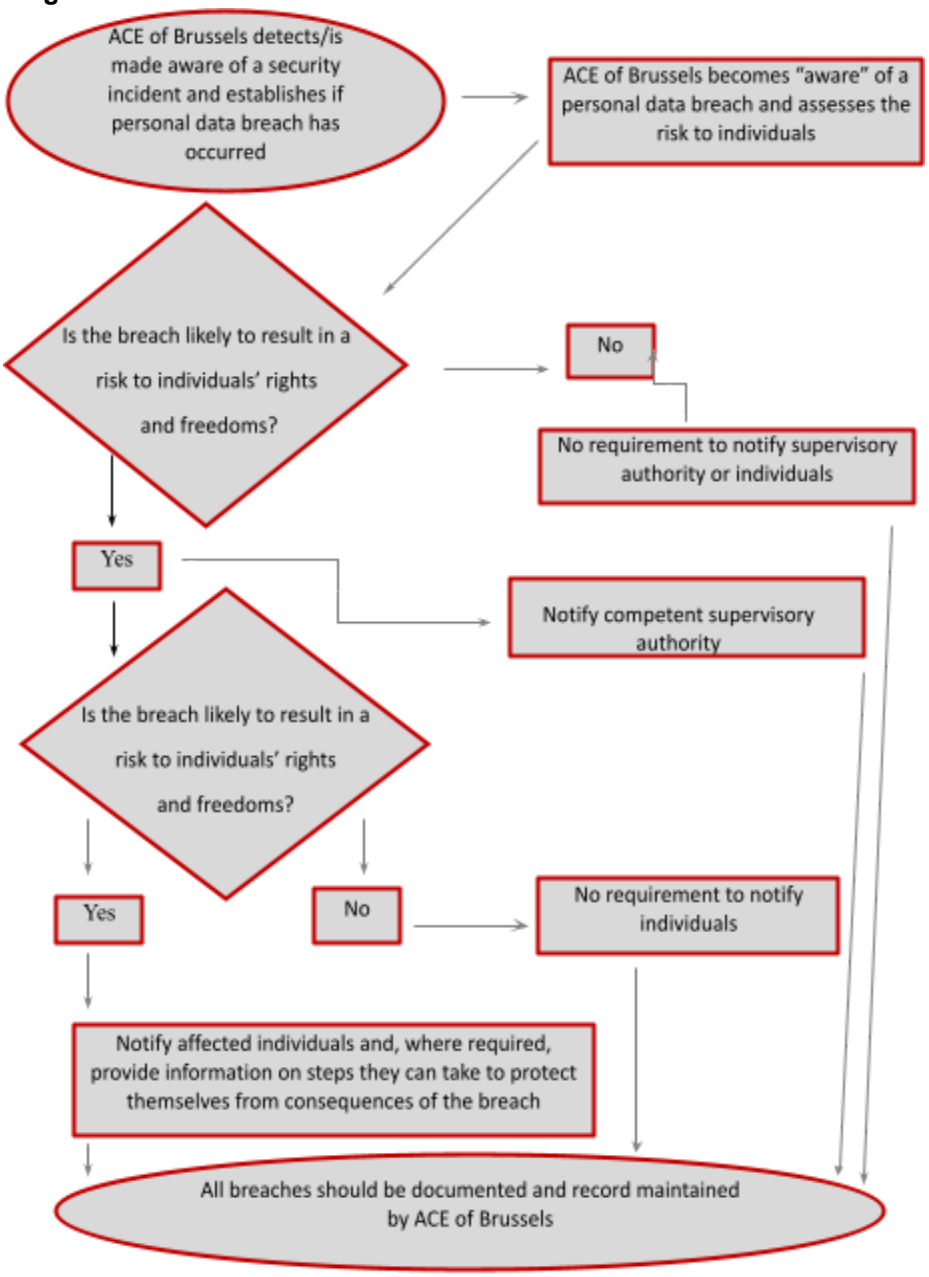
Advice from (external) experts may be sought in resolving the incident promptly and appropriately.

**1.6. Notification**

ACE of Brussels will subsequently make a decision based on the seriousness of the breach whether or not there is a legal requirement to notify the relevant Supervisory Authority.

When deciding whether the Supervisory Authority must be notified of a certain incident, and possibly the data subject(s) as well, the following assessments will be made:

### 1.7. Documenting breaches




### 1.8.

As mentioned in the schedule above, once the incident is contained and regardless of whether ACE of Brussels was notified of the breach or not, a thorough review of the incident will take place. The report will detail the root cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

## 16. SPECIFIC EMPLOYEE INSTRUCTIONS

Any and all individuals working at ACE of Brussels who, in the execution of their role, have access to personal data should be fully aware of the fact that non-compliance with this privacy policy may lead to serious negative consequences for the data subjects' private life as well for ACE of Brussels as a school itself (i.e. high penalties imposed by the Supervisory Authorities, reputation issues).

Therefore, ACE of Brussels expects from its employees that they:

- Respect and apply the principles of this Data Protection and Privacy Policy;
- Monitor the accuracy of personal data which are processed and inform the relevant department to rectify the personal data if inaccurate;
- Only collect and process those personal data which are necessary for the performance of their tasks;
- Make sure that the person with whom they are sharing information, is authorised to receive this information;
- Lock their office space if not present;
- Work with anonymous data if possible;
- Don't access any information of which they are aware that they don't have the right to access this information;
- Store professional files only in the electronic environment of ACE of Brussels and therefore not on the hard drive of their computer. ACE of Brussels' systems will be updated in order to mitigate against security risks. In addition, this will also prevent loss of data because a back-up of the data will be regularly made;
- Lock their computer with a strong password if they leave their computer unattended;
- Immediately take any printed documents containing personal data from the printer;
- Take all necessary precautions in order to prevent that data are stolen or lost (e.g. by forgetting a laptop/smartphone on the train, by theft of a laptop left unattended in the car, by leaving a computer unlocked);
- Immediately report any potential data breach to Mrs Jackie Daire (info@aceofbrussels.com)

## 17. Enforcement of this Policy, sanctions

ACE of Brussels will ensure that this Data Protection and Privacy Policy is observed and duly implemented. All persons who have access to personal data must comply with this Policy.

Violations of the applicable data protection legislation may lead to penalties and/or claims for damages imposed by the Supervisory Authority or the competent court, to ACE of Brussels. If these damages directly result from the failure by you to adhere to this policy, this will be addressed by taking necessary disciplinary actions, as mentioned in the works regulations, including but not limited to a dismissal.

## 18. Communication about the policy

ACE OF BRUSSELS will offer periodic training on this Data Protection and Privacy. Attendance to this training is compulsory.

In addition to the training on this Policy, ACE of Brussels will communicate this Policy to current and new employees by posting it on its intranet.

## 19. Modifications on the Policy

ACE of Brussels reserves the right to modify this Data Protection and Privacy Policy as needed, for example, to comply with changes in laws, regulations or requirements introduced by Supervisory Authorities. ACE of Brussels will inform the data subjects of any material changes in this Policy.

## 20. Applicable law and jurisdiction

This Policy and any disputes arising out of in relation to this Policy shall be exclusively governed by and construed in accordance with Belgian law. The courts of Brussels, Belgium, shall be exclusively competent for any disputes arising out of or in relation to this Policy.

# Data Retention Policy

## 1. Purpose, Scope, and Users

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within ACE of BRUSSELS (further: the “School”).

This Policy applies to all departments, processes, and systems in all countries in which the School conducts business and has dealings or other business relationships with third parties.

This Policy applies to all School officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

This policy applies to all information used at the School. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio
- Data generated by physical access control system.
-

## 2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection and Privacy Policy

## 3. Retention Rules

### 3.1.Retention General Principle

In the event, for any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

### 3.2.Retention General Schedule

The Data Protection Officer defines the time period for which the documents and electronic records should be retained through the Data Retention Schedule.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by the School to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceedings recognised under local law.

## 3.3.Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage lies with the Data Protection Officer.

## 3.4.Destruction of Data

The School and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data lies with the Data Protection Officer.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the School's Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevent the permanent loss of essential information of the School as a result of malicious or unintentional destruction of information – these controls are described in the School's IT Policy.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

## 3.5.Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection, the Data Protection Officer has the responsibility to ensure that each of the School's offices complies with this Policy. It is also the responsibility of the Data Protection Officer to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to the Data Protection Officer. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the School's reputation, personal injury, harm or loss. Non-compliance with this Policy by employees may therefore result in disciplinary action. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to School premises or

information, may result in termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

# 4. Document Disposal

## 4.1.Routine Disposal Schedule

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges / external costs;
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that acSchool documents but do not add any value;
- Message slips;
- Superseded address list, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded;

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

## 4.2.Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level II documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain any confidential information or personal data and are published School documents. These should be strip-shredded or disposed of through a recycling School and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

## 5. Validity and document management

| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
|---|---|---|---|---|
| Data Retention Schedule | Data Protection Officer's Google Drive | Data Protection Officer | Only authorised persons may access this document | Permanently |

The owner of this document is the Data Protection Officer who must check and, if necessary, update the document at least once a year.

## 6. Validity and document management

The owner of this document is the Data Protection Officer who must check and, if necessary, update the document at least once a year.

# 7. Appendices

Appendix – Data Retention Schedule

**Financial Records**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Payroll records | Seven years after audit | Finance |
| Supplier contracts | Seven years after contract is terminated | Finance |
| Chart of Accounts | Permanent | Finance |
| Fiscal Policies and Procedures | Permanent | Finance |
| Permanent Audits | Permanent | Finance |
| Financial statements | Permanent | Finance |
| General Ledger | Permanent | Finance |
| Investment records (deposits, earnings, withdrawals) | 7 years | Finance |
| Invoices | 7 years | Finance |

| | | |
|---|---|---|
| Cancelled checks | 7 years | Finance |
| Bank deposit slips | 7 years | Finance |
| Business expenses documents | 7 years | Finance |
| Check registers/books | 7 years | Finance |
| Property/asset inventories | 7 years | Finance |
| Credit card receipts | 3 years | Finance |
| Petty cash receipts/documents | 3 years | Finance |

**Business Records**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Article of Incorporation to apply for corporate status | Permanent | Finance |
| Board policies | Permanent | Finance |
| Board meeting minutes | Permanent | Finance |

| | | |
|---|---|---|
| Tax or employee identification number designation | Permanent | Finance |
| Office and team meeting minutes | Permanent | Finance |
| Annual corporate filings | Permanent | Finance |

**HR: Employee Records**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals | As per legal requirement | HR |
| Applications for jobs, interview notes – Recruitment/promotion panel Internal Where the candidate is unsuccessful. | Deleted immediately | HR |
| Where the candidate is successful. | 7 years after employment ends | HR |
| Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies | 7 years | HR |

| | | |
|---|---|---|
| Bank details – current | Duration of employment | HR |
| Payrolls/wages | Duration of employment | HR |
| Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters | As per legal requirement | HR |
| Employee address details | 7 years after employment ends | HR |
| Expense claims | As per legal requirement | HR |
| Annual leave records | 7 years after employment ends | HR |
| Accident books<br><br>Accident reports and correspondence | 7 years after employment ends | HR |
| Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms | As per legal requirement | HR |
| Pregnancy/childbirth certification | As per legal requirement | HR |

| | | |
|---|---|---|
| Parental leave | As per legal requirement | HR |
| Maternity pay records and calculations | As per legal requirement | HR |
| Redundancy details, payment calculations, refunds, notifications | As per legal requirement | HR |
| Training and development records | Duration of employment | HR |

**Contracts**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Signed | As per legal requirement | Finance |
| Contract amendments | As per legal requirement | Finance |
| Successful tender documents | As per legal requirement | Finance |
| Unsuccessful tenders' documents | As per legal requirement | Finance |

| | | |
|---|---|---|
| Tender – user requirements, specification, evaluation criteria, invitation | As per legal requirement | Finance |
| Contractors' reports | As per legal requirement | Finance |
| Operation and monitoring, eg complaints | As per legal requirement | Finance |

**Parent and Child Data**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Platform data – inclusive of Video data, comments, attachments, profile picture, email address, first and second name | 30 Years | Office |
| Live chat history | 30 years | Office |
| Screen recordings from support session | 30 Years | Support |
| CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries, DPO information | 30 Years | Support |

| | | |
|---|---|---|
| Metrics data | Retained whilst person remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be anonymised | Development Team |

**Non – Customer Data**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Name, email address | Kept until person unsubscribes / requests to be removed from system or otherwise withdraws his/her consent | Office |
| Call recordings | Automatically deleted after 6 months unless for legal reasons | Office |

**IT**

| Personal data record category | Mandated retention period | Record owner |
|---|---|---|
| Recycle Bins | Cleared monthly | Individual employee |

| | | |
|---|---|---|
| Downloads | Cleared monthly | Individual employee |
| Inbox | All emails containing PII attachments deleted after 3 years. | Individual employee |
| Deleted Emails | Cleared monthly | Individual employee |
| Personal Network Drive | Reviewed quarterly, any documents containing PII deleted after 3 years | Individual employee |
| Local Drives & files | Moved to network drive monthly, then deleted from local drive | Individual employee |
| Google Drives | Reviewed quarterly, any documents containing PII deleted after 3 years | Individual employee |